بسم الله الرحمن الرحيم

Firewall system

ده بيفلتر الداتا اللى داخله واللى خارجه من الشبكة

وده ممكن يكون

defult permitبيسمح لكل حاجة انها تعدى عليه

والعكس defult denies

ولازم تتحقق شوية خصائص فى الfirewall

Always invoked

يعنى اى حد هيدخل على الشبكه لازم يعدى الاول ع الفايروول

tamperproof

يعنى احنا منقدرش نعدل فيه

types of firewall

1-packet filtering

هنا هو بيبص ع ال ip or protocol

يعنى ممكن امنع اى بى معين او مثلا اقفل بروتوكول مثلا زى التلنت واسيب ال http

فهنا هو بيدى فكره ال virtual lan

ان الشبكة الواحده اقسمها شبكتين الاتنين مش شايفين بعض مع انهم فى نفس الشكبة الكبيرة

فلو حد من الشبكة الاولى عاوز يبعت للشبكة التانية لازم

يروح الراوتر الاول وهنا هحط الفايرووول ع الروتر
هنا ممكن يحصل مشكله ممكن واحد ييجى على الراوتر
ويغير ال nexthop فى routing table

2-stateful inspection firewall
هنا الداتا عمرها ما بتوصل مع بعض ولكن بتوصل باكيت
باكيت وهى من اسمها statefulيعنى حاله بحاله لا فيه
بعض الاتاكر بيخلوا الباكيت صغيره بحيث ان الفايرووول
ميعرفش يجيبها وبردو ..فهنا بيتتبع الباكيت كلها عشان
يتاكد ان محصلهاش اختراق وهنا مش بيشوف الكونتنت بتاع
الباكيت

3-application proxy
ده مثلا بيراقب عدد الكراكتر او مثلا يسمحلك بنسبة داونلود
معينه وبردو من وظيفته ان لو فيه سورس خارج الشبكة
وعاوز يبعت لحد داخل الشبكة او مثلا واحد بره الجامعه
عاوز يبعت لواحد جوه الفايرووول بيتاكد ان الرساله المبعوته
اتبعتت للdestination الصح
4-guard
هنا هيبقى ليه القدرة انه يعمل كل الحاجات اللى فاتت زى
انه يعد الكراكتر از يشوف ال inside and outside
بجانب انه هيقرا الداتا المكتوبه زى مثلا برنامج زى الفايير
لو هما عاوزين يتجسسوا على اجهزة الموبيل مش معقول
هيسجلوا مكالمات العالم كله لا هما هنا هيقوله لو لقيت كلمه
معينه مكتوبة او الشخص يقولها سجلى المكالمه

Methods of attacks

1-brute force and directionary

ال brute force

ده بيعمل تخمي للباسورد عن طريق انه يجرب كل الارقام وكل الحروف فالاجهزة الحديثه وسرعتها العالية العملية دى بتبقى سريعة

اما ال dictionary attack

وظيفته انه بيخمن الباسورد يعنى مثلا لو الشخص عرف ان انا داخل ع السيستم ممكن يخمن الابسورد باسمى او بتاريخ ميلادى او رقم الموبايل وهكذا guessing technique

وعشان احمى نفسى لازم اعمل شوية حاجات كده

اول حاجة لازم اخد بالى من نظام المراقبه ممكن واحد قاعد جمبى ياخد الباسورد

تانى حاجة انى اخلى بالى من ان اى حد يحط مثلا فلاشة او اى حاجة الكترونية

تالت حاجة مسبش اليوزر يكتب الباسورد بمزاجه ممكن اشترط عليه انه ميكونش اقل من 6 حروف وهكذا

رابع حاجة انه مش بس يحط يوزر نيم وباسورد لا دانا كمان اخليه يعمل عمليه تانية زى مثلا يجاوب على سؤال لان مفيش برنامج هيقدر يفهم زى الانسان فالبتالى انا كدا بتاكد ان اللى بيكتب يوزر مش برنامج بيجرب ارقام

خامس حاجة اعمل السيستم انه بعد كذا محاوله يقفل

سادس حاجة لو قدرت اخلى الباسورد متشفر بطريقة احسن يبقى قشطة

2-Denial of service

يعنى انه مش قادر يعمل اى ريسبونس لاى ترافيك وده ممكن يكون مقصود وممكن لأ

لو مش مقصود مثلا زى البرنتر تبقى معلقة فانا لو فى لان يبقى انا كده عملت ترافيك

وانت كده كمان ممكن تعطل البروسيسور بتاعك

فهنا انا احاول مثلا اعمل امر يشوفلى البرنتر شغاله ولأ

flooding

هو انى ببعت ترافيك فيسببلى DOS

فهنا انا هحاول اشوف مين اللى بيعمل كده وامنعه من الدخول للشبكة

distributed denial of service

لما افتح بى سى انا ممكن اعمل كانتى فيرس ممكن اعمل كأى برنامج عندك فانا هنا بعمل spoofing

طب هنا لو انا قفلت ال idهقفل ال idبتاع مين ولا مين !!!

distributed reflective denial of service

هيبعت ال update فيها control packet

A SYN flood

بيفضل السينكرونس يعمل 3way hand check طول ما السيشن مفتوحه

Smurf attack

السيرفر بيبعت unuseless data

PING OF DEATH ATTACK

بيبعت باكيت الكونتن بتاعها فيها buffer overflow ودى ممكن تسبب كراش

stream attack

باكيتس ملهاش اى معنى بتتبعت للports

teardrop

بتركز ع ال bugsمن نظام التشغيل

land attack

هو اخطر انواع الاتاك هيبعت اكتر من sync packet منتحله

spoofing attack

هنا انا ممكن انتحل ال macبتاع الجهاز وادخل على نتورك على اساس انى جهاز معين

Man in the middle

اقدر اقف ف النص عشان اعمل interrupt

hijack attack

انا مثلا لما اعمل لوجين بعد كه اللى بكتبه مش شايفه فانا فتحت السكة للهاكر وهو يتصرف براحته وهنا اليوزر والسيرفر مش عارفين اغلط من ايه

sniffer attack

عاوز يعرف معلومات بس مش عارف هيعمل بيها وده ملوش تاثير دلوقت لكن تاثيره بييجى بعدين

Spamming attack

بيبعت useless dataبشكل عشوائى زى الميل ممكن من كتر الاسبام اللى بتتبعت الميل يتقفل

crackers
شخص unauthorizedبيحاول يخترق السيستم

IDs
فى ال firewallكان لو فيه شخص بيعمل هاك بتوقفه انما هنا هو وظيفته يراقب ويبلغ السيستم لة فيه مشكله والسيستم يتصرف
idsهيراقب ال raw dataويشوف هى low level or hight
لو واحد عمل امر printفده يبقى lowجايز يكون غلط مش مقصود بس لو اتعملت تانى فمش هينساها وهيعمله analysisلو اتاكد ان فيه حاجة غلط يحطه ف ال high level وبعد ال reactionعليه

Types of ids
signature level
وده حاجات ثابته يعنى الناس بحثت وعرفت ان اللى يدخل اكتر من 3 مرات يتعمله بلوك مجيش اقول خليها 4 او 5
heuristic
بيعمل list or modelللاشياء المسموح بيها للدخول اللى مش ف ال listمش هيدخل

Host based ids

بيراقب ال activityالغير مرغوب فيها على ال pcوده

احسن من ال network based ids

network based ids

بيراقب الactivity الغير مرغوب فيها على النتورك